IRREGULAR WARFARE CENTER
INSIGHTS
Vol. 2, No. 7, August 2024

21st Century Threats Require 21st Century Deterrence

Soon after the defeat of Germany in 1945, the United States and the Soviet Union found themselves in a global struggle for power and influence. In contrast to previous great power competitions, which had often led to conventional armed conflict, nuclear weapons dramatically changed the risk calculus for both sides. Since combat operations between nuclear armed adversaries could lead to their mutual annihilation, geopolitical competition between them would now reserve military force for "coercion, intimidation, and deterrence."

This led to the United States adopting a formal deterrence policy. Its adoption was a significant change for military doctrine. As nuclear strategist Bernard Brodie noted, "thus far the chief purpose of our military establishment has been to win wars, from now on its chief purpose must be to avert them." Traditionally, there are two forms of deterrence: "deterrence by denial" and "deterrence by punishment." Deterrence by denial is premised on the ability to deter actions by creating the perception they are unlikely to succeed. Deterrence by punishment is premised on the ability to impose retaliatory costs—economic, military, political, or some combination—for an aggressive action which are higher than any plausible benefits. Effective deterrence by either denial or punishment is predicated on the explicit elaboration of clearly defined national interests, "red lines" to denote when these interests would be threatened, the capability to implement threatened punishment, the credibility of will to follow through, and the ability to communicate with adversaries so that they understand the consequences of a given course of action.

IRREGULAR THREATS AND DETERRENCE

Cold War deterrence was largely effective because strategic competition between great powers was kept beneath the threshold of overt inter-state war. However, nuclear deterrence also resulted in what Glenn Snyder described as the stability-instability paradox: "the more stable the nuclear balance, the more

DR. JIM DERLETH
IWC Subject Matter Expert
(Contractor, Valens Global)

COL JEFF PICKLER
Commander, First Infantry Division Artillery Brigade

IWC MISSION: The IWC serves as the central mechanism for developing the Department of Defense's (DOD) irregular warfare knowledge and advancing the Department's understanding of irregular warfare concepts and doctrine in collaboration with key allies and partners.

likely powers will engage in conflicts below the threshold of war." This was true during the Cold War and remains so today. A 1981 State Department report highlighted various irregular actions taken by the Soviet Union, including "control of the press in foreign countries; forgery of documents; rumors, altered facts, and lies; use of international and local front organizations; and the use of academic, political, economic, and media figures as collaborators to influence the policies of the nation." These efforts usually failed to achieve significant strategic impact due to the limitations of information technology at the time, in addition to the overall bi-polar geopolitical environment. Today, because of technology which allows states to directly target societal vulnerabilities they couldn't before, and increased economic interdependence, states are much more vulnerable to irregular tactics. For instance, both the Russian interference in the 2016 U.S. presidential election and the 2020 SolarWinds data breach show that adversaries can accomplish certain strategic objectives at low-cost and with a limited risk of credible attribution or escalation.

These changes notwithstanding, the American approach to deterrence remains largely the same as it was during the Cold War. Doctrinally, it focuses on the use of conventional and nuclear forces to deter and, if necessary, defeat a peer adversary on the battlefield. For example, the U.S. Army's current modernization efforts prioritize lethality, with billions of dollars being poured into long range precision fires, next-generation combat vehicles, vertical-lift platforms, and air and missile defense systems. Training and exercises continue to focus on closing with, and destroying, adversaries through precision firepower and maneuver. While capable conventional and modern nuclear forces are crucial for deterrence, the last 15 years have shown that they do not deter the use of cyber-attacks, proxies, disinformation campaigns, and other irregular tactics which dominate contemporary strategic competition. In contrast, American adversaries have incorporated changes in the operating environment into their military strategies. For example, Russian Chief of the General Staff Gerasimov noted that the "rules of war" had changed, "The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."

As Mark Galeotti similarly noted in his book, *The Weaponisation of Everything*, "the world is now more complex and above all more inextricably interconnected than ever before...Wars without warfare, non-military conflicts fought with all kinds of other means, from subversion to sanctions, memes to murder, may be becoming the new normal." This strategic environment undermines our outdated deterrence doctrine, with the result that: "the greatest strategic challenge of the current era is neither the return of great-power rivalries nor the spread of advanced weaponry. It is the decline of deterrence." Such a situation allows adversaries to act with virtual impunity in the "grey zone." To change this situation, the United States must shift the cost-benefit calculus of Russia and other adversaries. In other words, Washington must develop an deterrence strategy for irregular threats.

INTEGRATED DETERRENCE

Since adversaries are using lethal and non-lethal irregular tactics to achieve their objectives, U.S. national security requires the ability to deter these threats. In the 2021 Interim National Security Strategic Guidance, President Biden pledged to, "develop capabilities to better compete and deter gray-zone actions." Since taking office, Secretary of Defense Austin noted that the United States needed a new way of approaching deterrence which would "impose costs where necessary, while using all of our tools to lower the risk of escalation with our adversaries and respond to challenges below the level of armed conflict." This policy is called "integrated deterrence."

While Undersecretary of Defense for Policy Colin Kahl described integrated deterrence as informing "almost everything that we do...integrated across domains, so conventional, nuclear, cyber, space,

informational, across theaters of competition and potential conflict [and] integrated across the spectrum of conflict from high intensity warfare to the gray zone." Kahl noted that while deterrence has been the focus of U.S. strategy policy since the Cold War, it now has a different meaning: "we need to think about deterrence differently given the existing security environment, and the potential scenarios for conflict that we're trying to deter...The Department of Defense needs to have the capabilities and the concepts to deny the type of rapid fait accompli scenarios that we know potential adversaries are contemplating..."

While the components of integrated deterrence have yet to be fully elaborated into explicit doctrine, it should include both the ability to "punish" an aggressor state using irregular tactics and "deny" it the ability to significantly impact the target state. As with traditional, integrated deterrence requires identifying and communicating "red lines" to adversaries. These red lines should nevertheless concede the fact that a country cannot deter the full spectrum of irregular activity. Instead, the focus should be on the most dangerous, understanding that this might also provide an invitation to exploit lower-level vulnerabilities. After identifying the most salient irregular threats, states need to first attain the capability to punish an adversary. The guiding principle should be to focus on contingencies an adversary does not want to happen. In other words, targeted states must be able to identify an adversary's vulnerabilities on core interests. Importantly, the selected countermeasures can either be in kind—countering cyber with cyber—or responses can be taken outside the domain in which the action occurred. One example could be threatening financial sanctions in case of a cyber-attack. For smaller states, this could include coordinating the collective punishment of an aggressor by a group (such as the EU or NATO) of which it is a member.

The second component of an integrated deterrence strategy is the ability of target states to deny an adversary any benefits from an irregular attack. This can be done by improving societal resilience. The European Union defines resilience as "the capacity to withstand stress and recover, strengthened from challenges." Resiliency measures are generally low cost and fit within established risk management paradigms of national security. Since the nature of irregular threats—which are ambiguous, hard to detect, and difficult to attribute—makes deterrence by punishment difficult, it is crucial that states make themselves less vulnerable to them. A resiliency-based denial component of a comprehensive deterrence strategy allows states to make better use of their scarce resources through the identification and mitigation of societal vulnerabilities. Resiliency also strengthens the foundations of a deterrence strategy, namely communication, capability, and credibility. In summary, an integrated deterrence strategy should try and prevent adversarial states from using irregular tactics, while simultaneously mitigating their impact if used. This strategy would shrink the operational space for irregular actions and disincentivize their use.

CONCLUSION

Creating a strategy which deters potential adversaries from using irregular tactics, though both punishment and denial, will be an essential feature of a 21st century deterrence strategy. In the increasingly blurred space between peace and war, states must be able to clearly communicate to potential aggressors that their conventional, nuclear, and irregular threats will not succeed. Deterrence will only remain credible if the United States and its allies have the capability to clearly communicate their willingness to follow through on commitments to punish and deny adversarial irregular actions. In summary, the United States needs a 21st century deterrence strategy to deter 21st century threats.